**IT Applications, Ch 7, Information Management**

Threats to the integrity and security of data and information stored, communicated and disposed of by organisations.

Complete the following from p 270-

**Deliberate threats**

1. When does intentional damage occur?

It occurs when an individual or group deliberately sets out to cause problems within an information system.

1. Unauthorised access is both physical and logical. Explain what this means?
2. Computer Virus
   1. Describe the nature of this virus.

Its nature is to infect the machine just like a biological virus might infect a human.

* 1. What is the main purpose of a virus?

The nature of a virus is to affect the running of the PC in a manner unintended by the user.

* 1. What is meant by the term, payload?

Payload is the action that the virus is designed to carry out.

* 1. Describe a worm?

A worm is where the virus by automatically attaching themselves to email messages, then locating all email addresses in a victims email program and sending on more infected messages without the victims knowledge.

* 1. List the other types of viruses, p 272, fig. 7-10.

Boot infectors, executable, macro, time bomb, logic bomb, worm, Trojan horse, resident, polymorphic.

* 1. How do viruses mainly spread?

They mainly spread through an email file attachment or by the transfer of infected files on removable storage devices.

1. Hacking/Cracking
   1. Who is a hacker and what damage do they cause?

A hacker is a person who gains unauthorised access to an information system.

1. Tampering with files
   1. Describe how employees tamper with files.

Employees tamper with files by changing their salary amounts.

* 1. What is industrial sabotage?

Industrial sabotage is when companies invest in countries and find out the transmission of electronic communications is controlled by a corrupt government that threatens to deny access to the communications systems unless they pay large sums of money.

1. Information theft
   1. Why does this occur?

This occurs because organisations look for an edge over their competitors.

1. Vandalism of hardware
2. Theft of hardware

**Accidental threats**

1. User error
   1. List some common examples of user error.

Examples of common user error are copying an older version of a file over a newer version or formatting a disk that contains important data.

* 1. What processes are in place to limit user error.

Safeguards are in place to limit the amount of data lost by users.

1. Failure to follow file-management procedures
   1. List common errors of employees in saving files.
      * File extensions have been left off
      * Non-descriptive file names were used
      * Folders were improperly used.

**Technical Failure**

1. List some examples of technical failure.
   * + Breakage
     + Variation in electricity flow
     + Smoke
     + Fire
     + Water damage.

**Consequences of violating security and privacy measures, p 278**

1. List three important consequences if security measures are violated.

If security measure where violated consequences would be breaches of privacy, loss of intellectual property and loss of income due to unavailability of information or services.